

JOSEPH W. COTCHETT (SBN 36324)
jcotchett@cpmlegal.com
ANDREW F. KIRTLEY (SBN 328023)
akirtley@cpmlegal.com
GIA JUNG (SBN 340160)
gjung@cpmlegal.com
COTCHETT, PITRE & McCARTHY, LLP
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Telephone: (650) 697-6000
Facsimile: (650) 697-0577

THOMAS E. LOESER (CA SBN: 202724)
tloeser@cpmlegal.com
KARIN B. SWOPE *Pro Hac Vice Pending*
kswope@cpmlegal.com
COTCHETT, PITRE & McCARTHY, LLP
999 N. Northlake Way, Suite 215
Seattle, WA 98103
Telephone: (206) 802-1272
Facsimile: (650) 697-0577

*Attorneys for Plaintiffs David Vita, Daniel Mariscal,
Charles Fairchild, Faith Brown and the proposed
Class*

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

**DAVID VITA, DANIEL MARISCAL,
CHARLES FAIRCHILD and FAITH
BROWN**, on behalf of themselves and a class
of similarly situated persons,

Plaintiffs,

v.

AT&T, INC.,

Defendant.

NO.:

CLASS ACTION COMPLAINT

- 1. Negligence**
- 2. Negligence Per Se**
- 3. Gross Negligence**
- 4. Breach of Express Contracts**
- 5. Breach of Implied Contracts**
- 6. Breach of Implied Duty of Good Faith and Fair Dealing**
- 7. Unjust Enrichment (Alternative to Breach of Contract Claim)**
- 8. Declaratory Judgment**
- 9. Violation of the California Customer Records Act, Cal. Civ. Code §§1798.80, *Et Seq.***
- 10. Violation of the California Unfair Competition Law, Cal. Bus. & Prof.**

CLASS ACTION COMPLAINT

Code §§ 17200, *Et Seq.*

**11. Violation of the California Consumer
Legal Remedies Act, Cal. Civ. Code §§
1750, *Et Seq.***

**12. Violation of the California Consumer
Privacy Act, Cal. Civ. Code
§§1798.100. *Et Seq.***

JURY TRIAL DEMANDED

TABLE OF CONTENTS

		<u>Page</u>
1		
2		
3	I. INTRODUCTION	1
4	II. JURISDICTION, VENUE, AND CHOICE OF LAW	3
5	III. PARTIES	4
6	A. Plaintiff David Vita.....	4
7	B. Plaintiff Daniel Mariscal.....	6
8	C. Plaintiff Charles Fairchild.....	8
9	D. Plaintiff Faith Brown	10
10	E. Defendant.....	12
11	IV. FACTUAL BACKGROUND.....	12
12	A. AT&T Failed to Adequately Protect Customer Data, Resulting in	
13	the Data Breach.....	12
14	1. When first presented with evidence of the Data Breach, AT&T denied that	
15	it occurred.	12
16	2. Three years later, AT&T finally admits the Data Breach occurred.	13
17	B. The Data Breach Puts Consumers at Increased Risk of Fraud and	
18	Identity Theft	14
19	V. CLASS ACTION ALLEGATIONS	15
20	VI. CAUSES OF ACTION.....	17
21	<u>COUNT ONE</u> NEGLIGENCE	17
22	<u>COUNT TWO</u> NEGLIGENCE PER SE	19
23	<u>COUNT THREE</u> GROSS NEGLIGENCE.....	20
24	<u>COUNT FOUR</u> BREACH OF EXPRESS CONTRACTS.....	22
25	<u>COUNT FIVE</u> BREACH OF IMPLIED CONTRACTS.....	24
26	<u>COUNT SIX</u> BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR	
27	DEALING.....	26
28		

1	<u>COUNT SEVEN</u> UNJUST ENRICHMENT (ALTERNATIVE TO BREACH OF	
2	CONTRACT CLAIM).....	28
3	<u>COUNT EIGHT</u> DECLARATORY JUDGMENT	29
4	<u>COUNT NINE</u> VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS	
5	ACT, CAL. CIV. CODE §§ 1798.80, <i>ET SEQ.</i>	29
6	<u>COUNT TEN</u> VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION	
7	LAW, CAL. BUS. & PROF. CODE §§ 17200, <i>ET SEQ.</i>	31
8	<u>COUNT ELEVEN</u> VIOLATION OF THE CALIFORNIA CONSUMER LEGAL	
9	REMEDIES ACT, CAL. CIV. CODE §§ 1750, <i>ET SEQ.</i>	34
10	<u>COUNT TWELVE</u> VIOLATION OF THE CALIFORNIA CONSUMER	
11	PRIVACY ACT, CAL. CIV. CODE §§ 1798.100, <i>ET SEQ.</i>	37
12	VII. PRAYER FOR RELIEF	38
13	VIII. DEMAND FOR JURY TRIAL.....	39

1 Plaintiffs David Vita, Daniel Mariscal, Charles Fairchild and Faith Brown, individually
 2 and on behalf of all others similarly situated (“Plaintiffs”), bring this action against Defendant
 3 AT&T, Inc. (“AT&T” or “Defendant”), seeking monetary damages, restitution, and/or injunctive
 4 relief for the proposed Class, as defined below. Plaintiffs make the following allegations upon
 5 information and belief, the investigation of their counsel, and personal knowledge or facts that
 6 are a matter of public record.

7 I. INTRODUCTION

8 1. The release, disclosure, and publication of sensitive, private data can be
 9 devastating. Not only is it an intrusion of privacy and a loss of control, but it is a harbinger of
 10 identity theft: for victims of a data breach, the risk of identity theft more than quadruples.¹ A
 11 data breach can have grave consequences for victims for years after the actual date of the
 12 breach—with the obtained information, thieves can wreak many forms of havoc: open new
 13 financial accounts, take out loans, obtain medical services, obtain government benefits, and/or
 14 obtain driver’s licenses in the victims’ names, forcing victims to maintain a constant vigilance
 15 over the potential misuse of their information.

16 2. AT&T markets itself nationally as a sophisticated, reliable telephone, television,
 17 internet and cellular network provider that “take[s] cybersecurity very seriously and privacy is a
 18 fundamental commitment at AT&T.”² AT&T represents: “We use strong safeguards to keep
 19 your data safe and secure”³ and that at AT&T:

20 We work hard to safeguard your information using technology
 21 controls and organizational controls. We protect our computer
 22 storage and network equipment. We require employees to
 23 authenticate themselves to access sensitive data. We limit access to
 24 personal information to the people who need access for their jobs.

25 ¹ Dave Maxfield & Bill Latham, Data Breaches: Perspectives from Both Sides of the Wall, S.C. Lawyer (May
 26 2014).

27 ² *Keeping your account secure*, AT&T, <https://www.att.com/support/article/my-account/000101995?bypasscache=1/?source=EPcc000000000000U> (last visited Apr. 4, 2024).

28 ³ *Our Privacy Approach*. AT&T, <https://about.att.com/privacy.html> (last visited Apr. 4, 2024).

1 And we require callers and online users to authenticate themselves
2 before we provide account information.⁴

3 3. Despite these representations, AT&T seems incapable of adequately protecting
4 the information it maintains from and about its customers. Just last March (2023), AT&T
5 notified nine million wireless customers that their account information had been exposed. In
6 March of this year it announced a far larger data breach that impacts 73 million of its customers
7 across all of its communications services (the “Data Breach”).

8 4. What is extraordinarily troubling about the Data Breach is that it did not stem
9 from a recent intrusion. Rather, the Personally Identifying Information (PII) of some 7.6 million
10 current AT&T customers and 65.4 million former AT&T customers was likely stolen in 2018,
11 without AT&T ever detecting the intrusion or exfiltration of these huge amounts of data. This
12 fact alone portends that AT&T’s data security systems are woefully inadequate and at least
13 negligently monitored and controlled.

14 5. Since the intrusion and exfiltration of the PII of 73 million AT&T customers there
15 have been several listings, postings and descriptions of the pilfered data made available online
16 and reported to AT&T, yet in each instance AT&T denied that its systems had been breached.
17 Only in late March 2024, did AT&T finally admit this trove of PII came from its system and
18 began the process of notifying those tens of millions of affected consumers. All the while,
19 hackers and criminals have had access to this valuable information, exposing affected consumers
20 to severe risks of identity theft and financial fraud.

21 6. AT&T has admitted that hackers gained access to customer information and may
22 have obtained “full names, email addresses, mailing addresses, phone numbers, Social Security
23 Numbers, dates of birth, AT&T account numbers, and passcodes.”⁵

24 7. As a result of the Data Breach, through which their Personally Identifiable
25 Information (“PII”) was compromised, disclosed, and obtained by unauthorized third parties,

26
27 ⁴ AT&T Privacy Notice, <https://about.att.com/privacy/privacy-notice.html#data-retention> (last visited Apr. 4, 2024).

28 ⁵ See *supra*, N. 2..

1 Plaintiffs and Class Members have suffered concrete damages and are now exposed to a
2 heightened and imminent risk of fraud and identity theft for a period of years, if not decades.
3 Furthermore, Plaintiffs and Class Members must now and in the future closely monitor their
4 financial accounts to guard against identity theft, at their own expense. Consequently, Plaintiffs
5 and the other Class Members will incur ongoing out-of-pocket costs for, *e.g.*, purchasing credit
6 monitoring services, credit freezes, credit reports, or other protective measures to deter and
7 detect identity theft.

8 8. By this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves
9 and all similarly situated individuals whose Private Information was accessed during the Data
10 Breach.

11 II. JURISDICTION, VENUE, AND CHOICE OF LAW

12 9. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C.
13 § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C.
14 § 1711, *et seq.*, because at least one member of the Class, as defined below, is a citizen of a
15 different state than Defendant, there are more than 100 members of the Class, and the aggregate
16 amount in controversy exceeds \$5,000,000, exclusive of interest and costs. This Court also has
17 diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(a).

18 10. This Court has jurisdiction over Defendant AT&T, Inc. because AT&T, Inc. has
19 committed acts with this District giving rise to this action and has established minimum contacts
20 with this forum such that the exercise of jurisdiction over AT&T, Inc. would not offend
21 traditional notions of fair play and substantial justice. AT&T, Inc. has engaged in continuous,
22 systematic, and substantial activities within this State, including substantial marketing and sales
23 of services and products in connection with the Data Breach within this State.

24 11. This Court also has jurisdiction over Defendant because the AT&T Legal
25 Department is located in **San Francisco, California** and has been involved legally with AT&T’s
26 response to and delayed admission of the Data Breach.

27 12. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because at
28 least one plaintiff is domiciled in this District and (i) a substantial part of the events or omissions
CLASS ACTION COMPLAINT
CASE NO.

1 giving rise to the claims occurred in, was directed to, and/or emanated from this District; and (ii)
2 Defendant have significant operations in this District, including the AT&T Legal Department,
3 which on information and belief, was instrumental in formulating Defendant's response to the
4 Data Breach.

5 **III. PARTIES**

6 **A. Plaintiff David Vita**

7 13. Plaintiff David Vita is a citizen of and is domiciled in Mount Shasta, California.

8 14. Plaintiff is a current customer of AT&T for his landline and internet, television,
9 and cellular telephone services.

10 15. Plaintiff provided confidential and sensitive PII to AT&T, as requested and
11 required by AT&T for the provision of its services. AT&T obtained and continues to maintain
12 Plaintiff's PII and has a legal duty and obligation to protect that PII from unauthorized access
13 and disclosure.

14 16. Plaintiff would not have entrusted his PII to AT&T had he known that AT&T
15 failed to maintain adequate data security.

16 17. On or about April 2, 2024, Plaintiff received the following notification from
17 AT&T that his information was compromised:



Account Information
Account ending [REDACTED]

[REDACTED]
David Vita
[REDACTED]
Mount Shasta, CA [REDACTED]
[REDACTED]

Keeping Your Account Secure

April 2, 2024

Dear David,

We take cybersecurity very seriously and privacy is a fundamental commitment at AT&T. We have discovered that your AT&T account passcode has been compromised, therefore we have proactively reset your passcode.

Our internal teams are working with external cybersecurity experts to analyze the situation. It appears the data is from more than 4 years ago and does not contain personal financial information or call history.

What information was involved?

The information varied by customer and account, but may have included full name, email address, mailing address, phone number, social security number, date of birth, AT&T account number and passcode.

If your sensitive personal information was compromised, we will provide complimentary identity theft and credit monitoring services.

What is AT&T doing?

We've taken precautionary measures and reset your passcode, which is an extra layer of protection for your account. When you sign in to your online account or call customer care, we'll provide details to help you personalize your passcode.

What can you do?

In addition to resetting your AT&T passcode, we encourage customers to remain vigilant by monitoring account activity and credit reports. You can set up free fraud alerts from nationwide credit bureaus — Equifax, Experian, and TransUnion. You can also request and review your free credit report at any time via [Freecreditreport.com](https://freecreditreport.com).

More Information

Visit att.com/accountsafety for more information and updates.

We apologize this has happened and are committed to keeping your account secure.

AT&T

© 2024 AT&T Intellectual Property. All Rights Reserved. AT&T, Globe logo, and all other marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.
A2820304

18. Plaintiff subsequently spent several hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach, researching ways to protect himself

1 from data breaches, and reviewing his financial accounts for fraud or suspicious activity. He now
2 plans to spend several hours a month checking account statements for irregularities.

3 19. Plaintiff is particularly concerned about his banking information because he had
4 autopay set up with AT&T and, therefore, it has all of his bank account information, in addition
5 to the PII associated with his AT&T account.

6 20. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result
7 of the release of his PII, which he expected AT&T to protect from disclosure, including anxiety,
8 concern, and unease about unauthorized parties viewing and potentially using his PII. As a result
9 of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the
10 impact of the Data Breach.

11 **B. Plaintiff Daniel Mariscal**

12 21. Plaintiff Daniel Mariscal is a citizen of and is domiciled in the state of California.

13 22. Plaintiff is a present customer of AT&T for internet services and is a former
14 customer of AT&T for cellular telephone services.


15 23. Plaintiff provided confidential and sensitive PII to AT&T, as requested and
16 required by AT&T for the provision of its services. AT&T obtained and continues to maintain
17 Plaintiff's PII and has a legal duty and obligation to protect that PII from unauthorized access
18 and disclosure.

19 24. Plaintiff would not have entrusted his PII to AT&T had he known that AT&T
20 failed to maintain adequate data security.

21 25. On or about April 8, 2024, Plaintiff received the following notification from
22 Experian that his information was compromised:

Internet Surveillance04/08/2024X

Compromised Social Security Number



Monitored Social Security Number: [REDACTED]

Date Found:04/06/2024

Why am I receiving this?

Experian IdentityWorks monitors illegal internet sites on the dark web and notifies you if a match to your personal information is detected. Unfortunately, Your Social Security number (SSN) has been found on the dark web.

This does not mean you are a victim of identity theft. However, identity thieves can use your SSN in a variety of ways including to apply for credit in your name, file a fake tax return or obtain medical care. It can also be used to steal Social Security or unemployment benefits or provided to law enforcement in connection with a crime.

Additional Info

Details

Last Name	[REDACTED]	Phone Number	[REDACTED] 76
Address 1	[REDACTED]	Social Security	***-**- [REDACTED]
City	[REDACTED]	Number	
State	UT	Potential Site	AT&T DATA
Zip	[REDACTED]	Records Found	04/06/2024
		On	
		Found With	SOCIAL SECURITY NUMBER

What should I do now?

- Review all three of your credit reports for new activity, if available. If you see something you do not recognize, that is an indicator of potential identity theft
- Continuously monitor your credit reports for activity

Still unsure about what to do next?

[Contact Customer Care](#). We'll help you determine if identity theft has occurred and work with you to resolve it.

Thank you for choosing Experian IdentityWorks. We will continue to monitor your information and notify you if a match is found in the future.

26. Shortly thereafter, Plaintiff received the following additional notice from his Chase Journey credit monitoring service:

Data breach alert





Your personal information was exposed in a data breach. Take a closer look and get steps to help protect your identity.

INFORMATION FOUND

▼ Social Security number

Social Security number:	Exposed
Date information updated:	2024-04-06 06:12:05
Compromised website:	AT&T data

What you can do next

-  Contact the Social Security Administration at [1-800-772-1213](tel:1-800-772-1213) to let them know that your SSN was compromised. They'll tell you what to do to next.
-  Review your [credit report](#) for any activity you don't recognize.
-  Consider placing a [credit freeze](#) on your credit report with the three major credit bureaus as an additional precaution.
-  For extra safety, continue checking your ID monitoring alerts to keep track of new activity or changes.

27. Plaintiff subsequently spent several hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach, researching ways to protect himself from data breaches, and reviewing his financial accounts for fraud or suspicious activity. He now plans to spend several hours a month checking account statements for irregularities.

28. In addition, Plaintiff was forced to lock all of his credit reports, which requires him to individually unlock and then relocked them anytime he wishes to use his own credit.

29. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of his PII, which he expected AT&T to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his PII. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the impact of the Data Breach.

C. Plaintiff Charles Fairchild

30. Plaintiff Charles Fairchild is a citizen of and is domiciled in Pasadena, California.

1 31. Plaintiff is a former customer of AT&T for internet and satellite television
2 services.

3 32. Plaintiff provided confidential and sensitive PII to AT&T, as requested and
4 required by AT&T for the provision of its services. AT&T obtained and continues to maintain
5 Plaintiff's PII and has a legal duty and obligation to protect that PII from unauthorized access
6 and disclosure.

7 33. Plaintiff would not have entrusted his PII to AT&T had he known that AT&T
8 failed to maintain adequate data security.

9 34. On or about April 16, 2024, Plaintiff received the following notification from
10 AT&T that his information was compromised:

11 **AT&T Security Update**

12 **Hello,**

13
14
15 We're contacting you regarding the security of your data. After a thorough assessment, AT&T has
16 determined that some of your personal information was compromised. To the best of our knowledge,
17 the compromised data does **not** include personal financial information or call history.

18 **What is AT&T doing to help?**

19 AT&T takes these issues very seriously. We are offering you one year of complimentary credit
20 monitoring, identity theft detection and resolution services, provided by Experian's[®] IdentityWorksSM.
21 To get started with IdentityWorksSM, please follow the instructions below and **enroll by August 30,**
22 **2024.**

23 **Where can you get more information?**

24 Visit att.com/accountsafety for more details.

25 We apologize this has happened.

26 AT&T

27 35. Plaintiff subsequently spent several hours taking action to mitigate the impact of
28 the Data Breach, including researching the Data Breach, researching ways to protect himself

1 from data breaches, and reviewing his financial accounts for fraud or suspicious activity. He now
2 plans to spend several hours a month checking account statements for irregularities.

3 36. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result
4 of the release of his PII, which he expected AT&T to protect from disclosure, including anxiety,
5 concern, and unease about unauthorized parties viewing and potentially using his PII. As a result
6 of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the
7 impact of the Data Breach.

8 **D. Plaintiff Faith Brown**

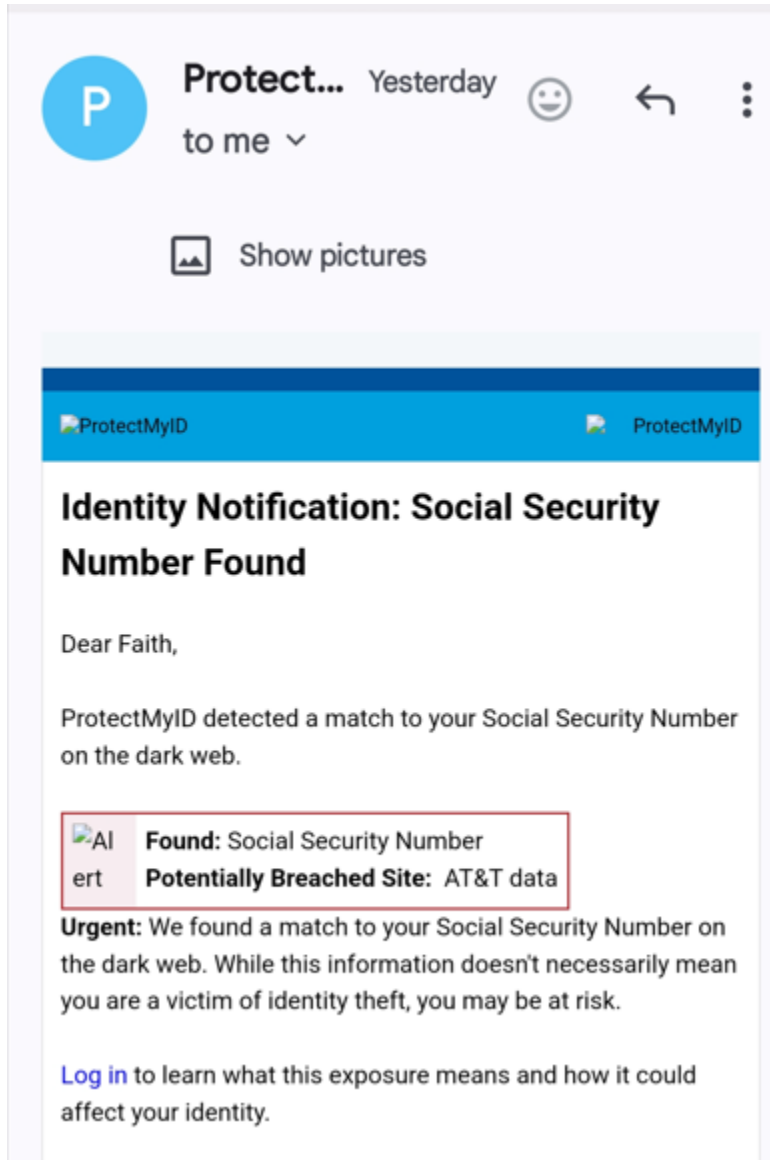
9 37. Plaintiff Faith Brown is a citizen of and is domiciled in Riverside in the state of
10 California.

11 38. Plaintiff is a former customer of AT&T.

12 39. Plaintiff provided confidential and sensitive PII to AT&T, as requested and
13 required by AT&T for the provision of its services. AT&T obtained and continues to maintain
14 Plaintiff's PII and has a legal duty and obligation to protect that PII from unauthorized access
15 and disclosure.

16 40. Plaintiff would not have entrusted her PII to AT&T had she known that AT&T
17 failed to maintain adequate data security.

18 41. On or about March 30, 2024, Plaintiff received the following notification from her
19 credit monitoring service:



42. Plaintiff subsequently spent several hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach, researching ways to protect herself from data breaches, and reviewing her financial accounts for fraud or suspicious activity. She now plans to spend several hours a month checking account statements for irregularities.

43. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of her PII, which he expected AT&T to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using her PII. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the impact of the Data Breach.

E. Defendant

44. Defendant AT&T, Inc. is a Delaware corporation with its principal place of business in Dallas, Texas. On information and belief, AT&T is the largest provider of landline and long-distance services in California. Also on information and belief, AT&T is the only available provider of internet service to millions of California residents and approximately 40 million AT&T cellular subscribers are domiciled in California.

45. The AT&T Legal Department, including on information and belief the employees responsible for Defendant's response to the Data Breach, are located at 430 Bush Street, in San Francisco, California.

46. In the course of its business, AT&T collects names, phone numbers, Social Security numbers, physical addresses, driver's license information, and other information from its customers and prospective customers.

IV. FACTUAL BACKGROUND

A. AT&T Failed to Adequately Protect Customer Data, Resulting in the Data Breach

1. When first presented with evidence of the Data Breach, AT&T denied that it occurred.

47. Customer PII from the Data Breach first appeared for sale nearly three years ago. In August 2021, ShinyHunters, a known criminal hacking group, posted for sale "AT&T Database +70M (SSN/DOB)" on a hacker forum and marketplace.⁶ ShinyHunters stated they would sell the database immediately for \$1 million.

48. Hackread, one of the technology sites that reported the auctioning of the data online noted:⁷

⁶ Waqas, AT&T breach? ShinyHunters selling AT&T database with 70 million SSN, HACKREAD (Aug. 20, 2021), <https://www.hackread.com/att-breach-shinyhunters-database-selling-70-million-ssn/>.

⁷ *Id.*

Hackread.com has seen the sample records shared by ShinyHunters on the forum and a quick review of it reveals that these records include the following customers' details:

- Full names
- Addresses
- Zipcodes
- Date of birth
- Email addresses
- Social security numbers (SSN)

49. AT&T learned of the auction of this data, but in response claimed that the data did not come from its servers.⁸

2. Three years later, AT&T finally admits the Data Breach occurred.

50. On March 17, 2024, MajorNelson provided free of charge on a hacking forum a database containing over 73 million records that appeared to contain AT&T customer information. Analysis showed that this database was the same set of information that had been offered for sale by ShinyHunters three years earlier.⁹

51. But this time, when faced with the same set of customer information that included AT&T account-specific information, the massive Data breach was no longer deniable by AT&T. AT&T admitted that its systems were compromised:

AT&T has determined that AT&T data-specific fields were contained in a data set released on the dark web approximately two weeks ago. While AT&T has made this determination, it is not yet known whether the data in those fields originated from AT&T or one of its vendors. With respect to the balance of the data set, which includes personal information such as social security numbers, the source of the data is still being assessed.

AT&T has launched a robust investigation supported by internal and external cybersecurity experts. Based on our preliminary analysis, the data set appears to be from 2019 or earlier, impacting

⁸ Lawrence Abrams, AT&T denies data breach after hacker auctions 70 million user database, BLEEPINGCOMPUTER (Aug. 20, 2021, 9:43 AM), <https://www.bleepingcomputer.com/news/security/atandt-denies-data-breach-after-hacker-auctions-70-million-user-database/>.

⁹ Lawrence Abrams, AT&T says leaked data of 70 million people is not from its systems, BLEEPINGCOMPUTER (Mar. 17, 2024, 7:24 PM), <https://www.bleepingcomputer.com/news/security/att-says-leaked-data-of-70-million-people-is-not-from-its-systems/>.

1 approximately 7.6 million current AT&T account holders and
2 approximately 65.4 million former account holders.

3 Currently, AT&T does not have evidence of unauthorized access to
4 its systems resulting in exfiltration of the data set. The company is
5 communicating proactively with those impacted and will be
6 offering credit monitoring at our expense where applicable. We
7 encourage current and former customers with questions to visit
8 www.att.com/accountsafety for more information.

9 As of today, this incident has not had a material impact on
10 AT&T's operations.¹⁰

11 52. After falsely denying its systems were breached in August 2021, AT&T appears
12 to have done nothing at all to protect its 73 million current and former customers from the effects
13 of its negligence for the following nearly three years. AT&T now claims to have “launched a
14 robust investigation supported by internal and external cybersecurity experts,” something it
15 should have done in 2021 to have any hope of actually mitigating the extensive harm its false
16 denial has—and no doubt will—cause for years to come.

17 53. AT&T was familiar with its obligations—created by contract, industry standards,
18 common law, and representations to its customers—to protect customer information. Plaintiffs
19 and Class Members provided their Private Information to AT&T with the reasonable expectation
20 that AT&T would comply with its obligations to keep such information confidential and secure.

21 54. AT&T failed to comply with these obligations, resulting in the Data Breach.
22 Plaintiffs and Class Members now face years of constant surveillance of their financial and
23 personal records.

24 **B. The Data Breach Puts Consumers at Increased Risk of Fraud and Identity Theft**

25 55. An identity thief uses victims' PII, such as name, address, and other sensitive and
26 confidential information, without permission, to commit fraud or other crimes that range from
27 immigration fraud, obtaining a driver's license or identification card, obtaining government
28 benefits, and filing fraudulent tax returns to obtain tax refunds.

¹⁰ *Id.*

56. Identity thieves can use a victim's PII to open new financial accounts, incur charges in the victim's name, take out loans in the victim's name, and incur charges on existing accounts of the victim. Plaintiffs' finances are now at risk due to the Data Breach.

57. Identity theft is the most common consequence of a data breach—it happens to 65% of data breach victims.¹¹ Consumers lost more than \$56 billion to identity theft and fraud in 2020, and over 75% of identity theft victims reported emotional distress.¹²

58. Plaintiffs are now in the position of having to take steps to mitigate the damages caused by the Data Breach. Once use of compromised non-financial PII is detected, the emotional and economic consequences to the victims are significant. Studies done by the ID Theft Resource Center, a non-profit organization, found that victims of identity theft had marked increased fear for personal financial security. The report attributes this to more people having been victims before, contributing to greater awareness and understanding that they may suffer long term consequences from this type of crime.¹³

59. AT&T failed to protect and safeguard Plaintiffs' and Class Members' private information, in fact failing to adhere to even its most basic obligations. As a result, Plaintiffs and Class Members have suffered or will suffer actual injury, including loss of privacy, costs, and loss of time.

V. CLASS ACTION ALLEGATIONS

60. Plaintiffs brings this action as a class action under Rule 23 of the Federal Rules of Civil Procedure, on behalf of a proposed nationwide class (the “Class”), defined as:

All natural persons in the State of California whose Personally Identifiable Information was compromised as a result of the Data Breach.

61. **Numerosity and Ascertainability:** Plaintiffs do not know the exact size of the Class or identity of the Class Members, since such information is in the exclusive control of

¹¹ Eugene Bekker, *What Are Your Odds of Getting Your Identity Stolen?*, IDENTITYFORCE (Apr. 15, 2021), <https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics> (last visited Feb. 1, 2023).

¹² *Id.*

¹³ Identity Theft: The Aftermath 2013, Identity Theft Resource Center, <https://idtheftinfo.org/latest-news/72> (last visited Feb. 1, 2023).

1 Defendant. Nevertheless, the data breach affected at least 73 million individuals dispersed
 2 throughout the United States. On information and belief, there are approximately 40 million
 3 AT&T subscribers in California whose information may have been compromised in the Data
 4 Breach. Also on information and belief, AT&T is the largest provider of phone and internet
 5 services in California and the only provider in many California communities. The number of
 6 Class Members is so numerous that joinder of all Class Members is impracticable. The names,
 7 addresses, and phone numbers of Class Members are identifiable through documents maintained
 8 by Defendant.

9 **62. Commonality and Predominance:** This action involves common questions of
 10 law and fact which predominate over any question solely affecting individual Class Members.
 11 These common questions include:

- 12 A. whether Defendant engaged in the conduct alleged herein;
- 13 B. whether Defendant had a legal duty to use reasonable security
 14 measures to protect Plaintiffs' and Class Members' PII;
- 15 C. whether Defendant timely, accurately, and adequately informed
 16 Plaintiffs and Class Members that their PII had been compromised;
- 17 D. whether Defendant breached its legal duty by failing to protect the
 18 PII of Plaintiffs and Class Members;
- 19 E. whether Defendant acted reasonably in securing the PII of
 20 Plaintiffs and Class Members;
- 21 F. whether Plaintiffs and Class Members are entitled to injunctive
 22 relief;
- 23 G. and whether Plaintiffs and Class Members are entitled to damages
 24 and equitable relief.

25 **63. Typicality:** Plaintiffs' claims are typical of the other Class Members' claims
 26 because all Class Members were comparably injured through Defendant's substantially uniform
 27 misconduct, as described above. Plaintiffs are advancing the same claims and legal theories on
 28 behalf of themselves and all other members of the Class that they represent, and there are no
 defenses that are unique to Plaintiffs. The claims of Plaintiffs and Class Members arise from the
 same operative facts and are based on the same legal theories.

64. **Adequacy:** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other members of the Class they seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation; and Plaintiffs intend to prosecute this action vigorously. The Class's interest will be fairly and adequately protected by Plaintiffs and their counsel.

65. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other detriment suffered by Plaintiffs and other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be virtually impossible for the Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not: individualized litigation creates a potential for inconsistent or contradictory judgments, increases the delay and expense to the parties, and increases the expense and burden to the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by this Court.

VI. CAUSES OF ACTION

COUNT ONE NEGLIGENCE

66. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

67. AT&T owed a duty to Plaintiffs and Class Members-arising from the sensitivity of the information, the expectation the information was going to be kept private, and the foreseeability of its data safety shortcomings resulting in an intrusion-to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, implementing, maintaining, monitoring, and testing AT&T's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class Members' information was adequately secured from unauthorized access.

1 68. AT&T's Privacy Notice acknowledged AT&T's duty to adequately protect
2 Plaintiffs' and Class Members' PII.

3 69. AT&T owed a duty to Plaintiffs and Class Members to implement administrative,
4 physical, and technical safeguards, such as intrusion detection processes that detect data breaches
5 in a timely manner, to protect and secure Plaintiffs' and Class Members' PII.

6 70. AT&T also had a duty to only maintain PII that was needed to serve customer
7 needs.

8 71. AT&T owed a duty to disclose the material fact that its data security practices
9 were inadequate to safeguard Plaintiffs' and Class Members' PII.

10 72. AT&T also had independent duties under California laws that required AT&T to
11 reasonably safeguard Plaintiffs' and Class Members' PII, and promptly notify them about the
12 Data Breach.

13 73. AT&T had a special relationship with Plaintiffs and Class Members as a result of
14 being entrusted with their PII, which provided an independent duty of care. Plaintiffs' and Class
15 Members' willingness to entrust AT&T with their PII was predicated on the understanding that
16 AT&T would take adequate security precautions. Moreover, AT&T was capable of protecting its
17 networks and systems, and the PII it stored on them, from unauthorized access.

18 74. AT&T breached its duties by, among other things: (a) failing to implement and
19 maintain adequate data security practices to safeguard Plaintiffs' and Class Members' PII,
20 including administrative, physical, and technical safeguards; (b) failing to detect the Data Breach
21 in a timely manner; and (c) failing to disclose that its data security practices were inadequate to
22 safeguard Plaintiffs' and Class Members' PII.

23 75. But for AT&T's breach of its duties, including its duty to use reasonable care to
24 protect and secure Plaintiffs' and Class Members' PII, Plaintiffs' and Class Members' PII would
25 not have been accessed by unauthorized parties.

26 76. Plaintiffs and Class Members were foreseeable victims of AT&T's inadequate
27 data security practices. AT&T knew or should have known that a breach of its data security
28 systems would cause damage to Plaintiffs and Class Members.

77. It was reasonably foreseeable that the failure to reasonably protect and secure Plaintiffs' and Class Members' PII would result in unauthorized access to AT&T's networks, databases, and computers that stored or contained Plaintiffs' and Class Members' PII.

78. As a result of AT&T's negligent failure to prevent the Data Breach, Plaintiffs and Class Members suffered injury, which includes, but is not limited to, exposure to a heightened and imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class Members have also incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter and detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also diminished the value of the PII.

79. The harm to Plaintiffs and Class Members was a proximate, reasonably foreseeable result of AT&T's breaches of its aforementioned duties.

80. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT TWO
NEGLIGENCE PER SE

81. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

82. Under the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45, AT&T had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs’ and Class Members’ PII.

83. In addition, under California data security statutes, AT&T had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' PII.

84. AT&T breached its duties to Plaintiffs and Class Members, under the Federal Trade Commission Act, 15 U.S.C. § 45, (“FTCA”) and California data security statutes, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs’ and Class Members’ PII.

1 85. Plaintiffs and Class Members were foreseeable victims of AT&T's violations of
2 the FTCA and California data security statutes. AT&T knew or should have known that its
3 failure to implement reasonable measures to protect and secure Plaintiffs' and Class Members'
4 PII would cause damage to Plaintiffs and Class Members.

5 86. AT&T's failure to comply with the applicable laws and regulations constitutes
6 negligence *per se*.

7 87. But for AT&T's violation of the applicable laws and regulations, Plaintiffs' and
8 Class Members' PII would not have been accessed by unauthorized parties.

9 88. As a result of AT&T's failure to comply with applicable laws and regulations,
10 Plaintiffs and Class Members suffered injury, which includes but is not limited to the exposure to
11 a heightened and imminent risk of fraud, identity theft, financial and other harm. Plaintiffs and
12 Class Members must monitor their financial accounts and credit histories more closely and
13 frequently to guard against identity theft. Plaintiffs and Class Members also have incurred, and
14 will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports,
15 credit freezes, credit monitoring services, and other protective measures to deter or detect
16 identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also
17 diminished the value of the PII.

18 89. The harm to Plaintiffs and the Class Members was a proximate, reasonably
19 foreseeable result of AT&T's breaches of the applicable laws and regulations.

20 90. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to
21 be proven at trial.

22 **COUNT THREE**
23 **GROSS NEGLIGENCE**

24 91. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

25 92. Plaintiffs and Class Members entrusted AT&T with highly-sensitive and
26 inherently personal private data subject to confidentiality laws.

27 93. In requiring, obtaining, and storing Plaintiffs' and Class Members' PII, AT&T
28 owed a duty of reasonable care in safeguarding the PII.

94. AT&T's networks, systems, protocols, policies, procedures, and practices, as described above, were not adequately designed, implemented, maintained, monitored, and tested to ensure that Plaintiffs' and Class Members' PII were secured from unauthorized access.

95. AT&T's networks, systems, protocols, policies, procedures, and practices, as described above, were not reasonable given the sensitivity of the Plaintiffs' and Class Members' private data and the known vulnerabilities of AT&T's systems.

96. AT&T did not comply with state and federal laws and rules concerning the use and safekeeping of this private data.

97. Upon learning of the Data Breach, AT&T should have immediately disclosed the Data Breach to Plaintiffs and Class Members, credit reporting agencies, the Internal Revenue Service, financial institutions, and all other third parties with a right to know and the ability to mitigate harm to Plaintiffs and Class Members as a result of the Data Breach.

98. Despite knowing its networks, systems, protocols, policies, procedures, and practices, as described above, were not adequately designed, implemented, maintained, monitored, and tested to ensure that Plaintiffs' and Class Members' PII were secured from unauthorized access, AT&T ignored the inadequacies and was oblivious to the risk of unauthorized access it had created.

99. AT&T's behavior establishes facts evidencing a reckless disregard for Plaintiffs' and Class Members' rights.

100. AT&T, therefore, was grossly negligent.

101. AT&T's negligence also constitutes negligence per se.

102. The negligence is directly linked to injuries.

103. As a result of AT&T's reckless disregard for Plaintiffs' and Class Members' rights by failing to secure their PII, despite knowing its networks, systems, protocols, policies, procedures, and practices were not adequately designed, implemented, maintained, monitored, and tested, Plaintiffs and Class Members suffered injury, which includes but is not limited to the exposure to a heightened, imminent risk of fraud, identity theft, financial, and other harm.

Plaintiffs and Class Members must monitor their financial accounts and credit histories more
CLASS ACTION COMPLAINT - 21
CASE NO.

1 closely and frequently to guard against identity theft. Plaintiffs and Class Members also have
2 incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining
3 credit reports, credit freezes, credit monitoring services, and other protective measures to deter or
4 detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also
5 diminished the value of the PII.

6 104. The harm to Plaintiffs and the Class Members was a proximate, reasonably
7 foreseeable result of AT&T's breaches of the applicable laws and regulations.

8 105. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to
9 be proven at trial.

10 **COUNT FOUR**
11 **BREACH OF EXPRESS CONTRACTS**

12 106. Plaintiffs reallege and incorporate by reference the allegations contained in each
13 of the preceding paragraphs as if fully set forth herein.

14 107. Plaintiffs and members of the Class, additionally and alternatively, allege that
15 they entered into valid and enforceable express contracts with AT&T.

16 108. Under these express contracts, AT&T promised and was obligated to: (a) provide
17 services to Plaintiffs and Class Members; and (b) protect Plaintiffs' and the Class Members' PII.
18 In exchange, Plaintiffs and members of the Class agreed to pay money for these services.

19 109. Both the provision of services, as well as the protection of Plaintiffs' and Class
20 Members' PII, were material aspects of these contracts.

21 110. AT&T's express representations, including, but not limited to, express
22 representations found in AT&T's Privacy Notice, formed an express contract requiring AT&T to
23 implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class
24 Members' PII.

25 111. Alternatively, the express contracts included implied terms requiring AT&T to
26 implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and
27 Class Members' PII, including in accordance with federal, state, and local laws, and industry
28 standards.

1 112. Consumers value their privacy, the privacy of their dependents, and the ability to
2 keep their PII associated with obtaining services private. To customers such as Plaintiffs and
3 Class Members, services that do not adhere to industry-standard data security protocols to protect
4 PII are fundamentally less useful and less valuable than services that adhere to industry-standard
5 data security. Plaintiffs and Class Members would not have entered into these contracts with
6 AT&T without an understanding that their PII would be safeguarded and protected.

7 113. A meeting of the minds occurred, as Plaintiffs and members of the Class provided
8 their PII to AT&T and paid for the provided services in exchange for, amongst other things,
9 protection of their PII.

10 114. AT&T materially breached the terms of these express contracts, including, but not
11 limited to, the terms stated in the relevant Privacy Notice. Specifically, AT&T did not comply
12 with federal, state, and local laws, or industry standards, or otherwise protect Plaintiffs' and the
13 Class Members' PII, as set forth above. Further, on information and belief, AT&T has not yet
14 provided Data Breach notifications to some affected Class Members who may already be victims
15 of identity fraud or theft or are at imminent risk of becoming victims of identity theft or fraud
16 associated with PII that they provided to AT&T. These Class Members are, as yet, unaware of
17 the potential source for the compromise of their PII.

18 115. The Data Breach was a reasonably foreseeable consequence of AT&T's actions in
19 breach of these contracts.

20 116. As a result of AT&T's failure to fulfill the data security protections promised in
21 these contracts, Plaintiffs and members of the Class did not receive the full benefit of the
22 bargain, and instead received services that were of a diminished value to that described in the
23 contracts. Plaintiffs and Class Members, therefore, were damaged in an amount at least equal to
24 the difference in the value of the secure services they paid for and the services they received.

25 117. Had AT&T disclosed that its security was inadequate or that it did not adhere to
26 industry-standard security measures, neither Plaintiffs, nor Class Members, nor any reasonable
27 person would have purchased services from AT&T.

1 118. As a result of AT&T's breach, Plaintiffs and Class Members suffered actual
2 damages resulting from the theft of their PII, as well as the loss of control of their PII, and
3 remain in imminent risk of suffering additional damages in the future.

4 119. As a result of AT&T's breach, Plaintiffs and the Class Members have suffered
5 actual damages resulting from their attempt to mitigate the effects of the breach of contract and
6 subsequent Data Breach, including but not limited to, taking steps to protect themselves from the
7 loss of their PII.

8 120. Accordingly, Plaintiffs and the other members of the Class have been injured as a
9 result of AT&T's breach of contracts and are entitled to damages and/or restitution in an amount
10 to be determined at trial.

11 **COUNT FIVE**
12 **BREACH OF IMPLIED CONTRACTS**

13 121. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

14 122. Plaintiffs and Class Members were required to provide their PII to obtain services
15 from AT&T. Plaintiffs and Class Members entrusted their PII to AT&T in order to obtain
16 services from them.

17 123. By providing their PII, and upon AT&T's acceptance of such information,
18 Plaintiffs and Class Members on one hand, and AT&T on the other hand, entered into implied
19 contracts for the provision of adequate data security, separate and apart from any express
20 contracts concerning the services provided, whereby AT&T was obligated to take reasonable
21 steps to secure and safeguard that information.

22 124. AT&T had an implied duty of good faith to ensure that the PII of Plaintiffs and
23 Class Members in its possession was only used in accordance with their contractual obligations.

24 125. AT&T was therefore required to act fairly, reasonably, and in good faith in
25 carrying out its contractual obligations to protect the confidentiality of Plaintiffs' and Class
26 Members' PII and to comply with industry standards, state laws, and regulations for the security
27 of this information, and AT&T expressly assented to these terms in its Privacy Notice as alleged
28 above.

1 126. Under these implied contracts for data security, AT&T was further obligated to
2 provide Plaintiffs and all Class Members with prompt and sufficient notice of any and all
3 unauthorized access and/or theft of their PII.

4 127. Plaintiffs and Class Members performed all conditions, covenants, obligations,
5 and promises owed to AT&T, including paying for the services provided by AT&T and/or
6 providing the PII required by AT&T.

7 128. AT&T breached the implied contracts by failing to take adequate measures to
8 protect the confidentiality of Plaintiffs' and Class Members' PII, resulting in the Data Breach.
9 AT&T unreasonably interfered with the contract benefits owed to Plaintiffs and Class Members.

10 129. Further, on information and belief, AT&T has not yet provided Data Breach
11 notifications to some affected Class Members who may already be victims of identity fraud or
12 theft, or are at imminent risk of becoming victims of identity theft or fraud, associated with the
13 PII that they provided to AT&T. These Class Members are unaware of the potential source for
14 the compromise of their PII.

15 130. The Data Breach was a reasonably foreseeable consequence of AT&T's actions in
16 breach of these contracts.

17 131. As a result of AT&T's conduct, Plaintiffs and Class Members did not receive the
18 full benefit of the bargain, and instead received services that were of a diminished value as
19 compared to the secure services they paid for. Plaintiffs and Class Members, therefore, were
20 damaged in an amount at least equal to the difference in the value of the secure services they
21 paid for and the services they received.

22 132. Neither Plaintiffs, nor Class Members, nor any reasonable person would have
23 provided their PII to AT&T had AT&T disclosed that its security was inadequate or that it did
24 not adhere to industry-standard security measures.

25 133. As a result of AT&T's breach, Plaintiffs and Class Members have suffered actual
26 damages resulting from theft of their PII, as well as the loss of control of their PII, and remain in
27 imminent risk of suffering additional damages in the future.

134. As a result of AT&T's breach, Plaintiffs and the Class Members have suffered actual damages resulting from their attempt to mitigate the effect of the breach of implied contract and subsequent Data Breach, including, but not limited to, taking steps to protect themselves from the loss of their PII. As a result, Plaintiffs and the Class Members have suffered actual identity theft and the ability to control their PII.

135. Accordingly, Plaintiffs and Class Members have been injured as a result of AT&T's breach of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT SIX
**BREACH OF IMPLIED DUTY OF
GOOD FAITH AND FAIR DEALING**

136. Plaintiffs reallege and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

137. Plaintiffs and Class Members entered into and/or were the beneficiaries of contracts with Defendant, as alleged above.

138. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations—both explicit and fairly implied—and would not impair the rights of the other parties to receive their rights, benefits, and reasonable expectations under the contracts. These included the covenants that Defendant would act fairly, reasonably, and in good faith in carrying out their contractual obligations to protect the confidentiality of Plaintiffs’ and Class Members’ PII and to comply with industry standards, federal and state laws, and regulations for the security of this information.

139. Special relationships exist between AT&T and Plaintiffs and Class Members. AT&T entered into special relationships with Plaintiffs and Class Members, who entrusted their confidential PII to AT&T and paid for services with AT&T.

140. AT&T promised and was obligated to protect the confidentiality of Plaintiffs' and Class Members' PII from disclosure to unauthorized third parties. AT&T breached the covenant

1 of good faith and fair dealing by failing to take adequate measures to protect the confidentiality
2 of Plaintiffs' and Class Members' PII, which resulted in the Data Breach. AT&T unreasonably
3 interfered with the contract benefits owed to Plaintiffs and Class Members by failing to
4 implement reasonable and adequate security measures consistent with industry standards to
5 protect and limit access to the PII of Plaintiffs and the Class in AT&T's possession.

6 141. Plaintiffs and Class Members performed all conditions, covenants, obligations,
7 and promises owed to AT&T, including paying AT&T for services and providing them the
8 confidential PII required by the contracts.

9 142. As a result of AT&T's breach of the implied covenant of good faith and fair
10 dealing, Plaintiffs and Class Members did not receive the full benefit of their bargain—services
11 with reasonable data privacy—and instead received services that were less valuable than what
12 they paid for and less valuable than their reasonable expectations under the contracts. Plaintiffs
13 and Class Members have suffered actual damages in an amount equal to the difference in the
14 value between services with reasonable data privacy that Plaintiffs and Class Members paid for,
15 and the services they received without reasonable data privacy.

16 143. As a result of AT&T's breach of the implied covenant of good faith and fair
17 dealing, Plaintiffs and Class Members have suffered actual damages resulting from the theft of
18 their PII and remain at imminent risk of suffering additional damages in the future.

19 144. As a result of AT&T's breach of the implied covenant of good faith and fair
20 dealing, Plaintiffs and Class Members have suffered actual damages resulting from their attempt
21 to ameliorate the effect of the Data Breach, including, but not limited to, taking steps to protect
22 themselves from the loss of their PII.

23 145. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class
24 Members suffered injury in fact and are therefore entitled to relief, including restitution,
25 declaratory relief, and a permanent injunction enjoining AT&T from its conduct. Plaintiffs also
26 seeks reasonable attorneys' fees and costs under applicable law.

COUNT SEVEN
UNJUST ENRICHMENT
(ALTERNATIVE TO BREACH OF CONTRACT CLAIM)

146. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

147. Plaintiffs and Class Members conferred a monetary benefit on AT&T in the form of monetary payments—directly or indirectly—for services received.

148. AT&T collected, maintained, and stored the PII of Plaintiffs and Class Members and, as such, AT&T had knowledge of the monetary benefits conferred by Plaintiffs and Class Members.

149. The money that Plaintiffs and Class Members paid to AT&T should have been used to pay, at least in part, for the administrative costs and implementation of data management and security. AT&T failed to implement—or adequately implement—practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

150. As a result of AT&T’s failure to implement security practices, procedures, and programs to secure sensitive PII, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in the value between services with reasonable data privacy that Plaintiffs and Class Members paid for, and the services they received without reasonable data privacy.

151. Under principles of equity and good conscience, AT&T should not be permitted to retain money belonging to Plaintiffs and Class Members because AT&T failed to implement the data management and security measures that are mandated by industry standards and that Plaintiffs and Class Members paid for.

152. AT&T should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds received by AT&T. A constructive trust should be imposed upon all unlawful and inequitable sums received by AT&T traceable to Plaintiffs and the Class.

COUNT EIGHT
DECLARATORY JUDGMENT

153. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

154. Plaintiffs and the Class have stated claims against AT&T based on negligence, negligence per se, gross negligence and negligent misrepresentation, and violations of various state and federal statutes.

155. AT&T failed to fulfill their obligations to provide adequate and reasonable security measures for the PII of Plaintiffs and the Class, as evidenced by the Data Breach.

156. As a result of the Data Breach, AT&T's system is more vulnerable to unauthorized access and requires more stringent measures to be taken to safeguard the PII of Plaintiffs and the Class going forward.

157. An actual controversy has arisen in the wake of the Data Breach regarding AT&T's current obligations to provide reasonable data security measures to protect the PII of Plaintiffs and the Class. AT&T maintains that its security measures were—and still are—reasonably adequate and denies that they previously had or have any obligation to implement better safeguards to protect the PII of Plaintiffs and the Class.

158. Plaintiffs seek a declaration that AT&T must implement specific additional, prudent industry security practices to provide reasonable protection and security to the PII of Plaintiffs and the Class. Specifically, Plaintiffs and the Class seek a declaration that AT&T's existing security measures do not comply with their obligations, and that AT&T must implement and maintain reasonable security measures on behalf of Plaintiffs and the Class to comply with their data security obligations.

COUNT NINE
VIOLATION OF THE
CALIFORNIA CUSTOMER RECORDS ACT,
CAL. CIV. CODE §§ 1798.80, *ET SEQ.*

159. Plaintiffs, individually and on behalf of the Class, incorporate all foregoing factual allegations as if fully set forth herein.

1 160. “[T]o ensure that Personal Information about California residents is protected,”
2 the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business
3 that “owns, licenses, or maintains Personal Information about a California resident shall
4 implement and maintain reasonable security procedures and practices appropriate to the nature of
5 the information, to protect the Personal Information from unauthorized access, destruction, use,
6 modification, or disclosure.”

7 161. AT&T is a business that owns, maintains, and licenses “personal information”,
8 within the meaning of Cal. Civ. Code § 1798.81.5(d)(1), about Plaintiffs and Class members.

9 162. On information and belief, AT&T is registered as a “data broker” in California,
10 which is defined as a “business that knowingly collects and sells to third parties the personal
11 information of a consumer with whom the business does not have a direct relationship.” Cal. Civ.
12 Code § 1798.99.80.¹⁴

13 163. Businesses that own or license computerized data that includes personal
14 information, including SSNs, are required to notify California residents when their personal
15 information has been acquired (or is reasonably believed to have been acquired) by unauthorized
16 persons in a data security breach “in the most expedient time possible and without unreasonable
17 delay.” Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification
18 must include “the types of Personal Information that were or are reasonably believed to have
19 been the subject of the breach.” Cal. Civ. Code § 1798.82.

20 164. AT&T is a business that owns or licenses computerized data that includes
21 personal information as defined by Cal. Civ. Code § 1798.82(h).

22 165. Plaintiffs’ and Class members’ Private Information includes “personal
23 information” as covered by Cal. Civ. Code §§ 1798.81.5(d)(1), 1798.82(h).

24 166. Because AT&T reasonably believed that Plaintiffs’ and Class members’ Private
25 Information was acquired by unauthorized persons during the Data Breach, AT&T had an
26
27

28 ¹⁴ <https://oag.ca.gov/data-broker/registration/185724>.

1 obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ.
2 Code § 1798.82.

3 167. By failing to disclose the Data Breach in a timely and accurate manner, AT&T
4 violated Cal. Civ. Code § 1798.82.

5 168. As a direct and proximate result of AT&T's violations of the Cal. Civ. Code
6 §§ 1798.81.5 and 1798.82, Plaintiffs and Class members suffered damages, as described above.

7 169. Plaintiffs and Class members seek relief under Cal. Civ. Code § 1798.84,
8 including actual damages and injunctive relief.

9
10 **COUNT TEN**
11 **VIOLATION OF THE**
12 **CALIFORNIA UNFAIR COMPETITION LAW,**
13 **CAL. BUS. & PROF. CODE §§ 17200, *ET SEQ.***

14 170. Plaintiffs, individually and on behalf of the Class, incorporate all foregoing
15 factual allegations as if fully set forth herein.

16 171. AT&T is a "person" as defined by Cal. Bus. & Prof. Code §17201.

17 172. AT&T violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in
18 unlawful, unfair, and deceptive business acts and practices.

19 173. AT&T's "unfair" and "deceptive" acts and practices include:

- 20 a) Failing to implement and maintain reasonable security and privacy measures to protect
21 Plaintiffs' and the Class Members' Private Information, which was a direct and
22 proximate cause of the Data Breach;
23 b) Failing to identify foreseeable security and privacy risks, remediate identified security
24 and privacy risks, and adequately improve security and privacy measures following
25 previous cybersecurity incidents, which was a direct and proximate cause of the Data
26 Breach;
27 c) Failing to comply with common law and statutory duties pertaining to the security and
28 privacy of Plaintiffs' and the Class Members' Private Information, including duties
imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the
Data Breach;

- d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and the Class Members' Private Information, including by implementing and maintaining reasonable security measures;
- e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f) Failing to timely and adequately notify Plaintiffs and the Class Members of the Data Breach;
- g) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and the Class Members' Private Information; and
- h) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

174. AT&T has engaged in "unlawful" business practices by violating multiple laws, including the CCRA, Cal. Civ. Code §§ 1798.80, *et seq.*, the CLRA, Cal. Civ. Code §§ 1780, *et seq.*, 15 U.S.C. § 680, *et seq.*, the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

175. AT&T's unlawful practices include:

- a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and the Class Members' Private Information, which was a direct and proximate cause of the Data Breach;
- b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- 1 c) Failing to comply with common law and statutory duties pertaining to the security and
2 privacy of Plaintiffs' and the Class Members' Private Information, including duties
3 imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, 15
4 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505,
5 and the CMIA, Cal. Civ. Code § 56.36(b), which was a direct and proximate cause of the
6 Data Breach;
- 7 d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and the
8 Class Members' Private Information, including by implementing and maintaining
9 reasonable security measures;
- 10 e) Misrepresenting that it would comply with common law and statutory duties pertaining to
11 the security and privacy of Plaintiffs' and the Class Members' Private Information,
12 including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15
13 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C.
14 §§ 6501- 6505, and the CMIA, Cal. Civ. Code § 56.36(b);
- 15 f) Failing to timely and adequately notify the Plaintiffs and the Class Members of the Data
16 Breach;
- 17 g) Omitting, suppressing, and concealing the material fact that it did not reasonably or
18 adequately secure Plaintiffs' and the Class Members' Private Information; and
- 19 h) Omitting, suppressing, and concealing the material fact that it did not comply with
20 common law and statutory duties pertaining to the security and privacy of Plaintiffs' and
21 the Class Members' Private Information, including duties imposed by the CLRA, Cal.
22 Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801,
23 *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA,
24 Cal. Civ. Code § 56.36(b).

25 176. AT&T's representations and omissions were material because they were likely to
26 deceive reasonable consumers about the adequacy of AT&T's data security and ability to protect
27 the confidentiality of consumers' Private Information.
28

1 177. AT&T's representations and omissions were material because they were likely to
2 deceive reasonable consumers, including Plaintiffs and the Class members, into believing that
3 their Private Information was secure.

4 178. As a direct and proximate result of AT&T's unfair, unlawful, and fraudulent acts
5 and practices, Plaintiffs and Class members were injured and lost money or property, including
6 monetary damages from fraud and identity theft, time and expenses related to monitoring their
7 financial accounts for fraudulent activity, an increased and imminent risk of fraud and identity
8 theft, and loss of value of their Private Information, including, but not limited to, the
9 diminishment of their present and future property interest in their Private Information and the
10 deprivation of the exclusive use of their Private Information.

11 179. AT&T acted intentionally, knowingly, and maliciously to violate California's
12 Unfair Competition Law, and recklessly disregarded Plaintiffs and Class members' rights.

13 180. Plaintiffs and Class members seek all monetary and non-monetary relief allowed
14 by law, including restitution of all profits stemming from AT&T's unfair, unlawful, and
15 fraudulent business practices or use of their Private Information; declaratory relief; reasonable
16 attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief;
17 and other appropriate equitable relief.

18 **COUNT ELEVEN**
19 **VIOLATION OF THE**
20 **CALIFORNIA CONSUMER LEGAL REMEDIES ACT,**
21 **CAL. CIV. CODE §§ 1750, *ET SEQ.***

22 181. Plaintiffs, individually and on behalf of the Class, incorporate all foregoing
23 factual allegations as if fully set forth herein.

24 182. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA")
25 is a comprehensive statutory scheme that is to be liberally construed to protect consumers against
26 unfair and deceptive business practices in connection with the conduct of businesses providing
27 goods, property, or services to consumers primarily for personal, family, or household use.

28 183. AT&T is a "person" as defined by Civil Code §§ 1761(c) and 1770, and has
provided "services" as defined by Civil Code §§ 1761(b) and 1770.

1 184. Plaintiffs and the Class are “consumers” as defined by Civil Code §§ 1761(d) and
2 1770, and have engaged in a “transaction” as defined by Civil Code §§ 1761(e) and 1770.

3 185. AT&T’s acts and practices were intended to and did result in the sales of products
4 and services to Plaintiffs and the Class members in violation of Civil Code § 1770, including:

- 5 a) Representing that goods or services have characteristics that they do not have;
- 6 b) Representing that goods or services are of a particular standard, quality, or grade when
7 they were not;
- 8 c) Advertising goods or services with intent not to sell them as advertised; and
- 9 d) Representing that the subject of a transaction has been supplied in accordance with a
10 previous representation when it has not.
- 11 e) AT&T violated Civil Code § 1770, in the following ways:
- 12 f) Failing to implement and maintain reasonable security and privacy measures to protect
13 Plaintiffs and Class members’ Private Information, which was a direct and proximate
14 cause of the Data Breach;
- 15 g) Failing to identify foreseeable security and privacy risks, remediate identified security
16 and privacy risks, and adequately improve security and privacy measures following
17 previous cybersecurity incidents, which was a direct and proximate cause of the Data
18 Breach;
- 19 h) Failing to comply with common law and statutory duties pertaining to the security and
20 privacy of Plaintiffs and Class members’ Private Information, including duties imposed
21 by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d., COPPA, 15 U.S.C.
22 §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b), which was a direct and
23 proximate cause of the Data Breach;
- 24 i) Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and
25 Class members’ Private Information, including by implementing and maintaining
26 reasonable security measures;
- 27 j) Misrepresenting that it would comply with common law and statutory duties pertaining to
28 the security and privacy of Plaintiffs and Class members’ Private Information, including

1 duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15
2 U.S.C. §§ 6501- 6505, and the CMIA, Cal. Civ. Code § 56.36(b);

3 k) Failing to timely and adequately notify the Plaintiffs and Class members of the Data
4 Breach;

5 l) Omitting, suppressing, and concealing the material fact that it did not comply with
6 common law and statutory duties pertaining to the security and privacy of Plaintiffs and
7 Class members' Private Information, including duties imposed by the FTC Act, 15
8 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C.
9 §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

10 186. AT&T's representations and omissions were material because they were likely to
11 deceive reasonable consumers about the adequacy of AT&T's data security and ability to protect
12 the confidentiality of consumers' Private Information.

13 187. Had AT&T disclosed to Plaintiffs and Class members that its data systems were
14 not secure and, thus, vulnerable to attack, AT&T would have been unable to continue in business
15 and it would have been forced to adopt reasonable data security measures and comply with the
16 law. Instead, AT&T was trusted with sensitive and valuable Private Information regarding
17 millions of consumers, including Plaintiffs, the Class, and the Class. AT&T accepted the
18 responsibility of being a steward of this data while keeping the inadequate state of its security
19 controls secret from the public. Accordingly, because AT&T held itself out as maintaining a
20 secure platform for Private Information data, Plaintiffs, the Class, and the Class members acted
21 reasonably in relying on AT&T's misrepresentations and omissions, the truth of which they
22 could not have discovered.

23 188. As a direct and proximate result of AT&T's violations of California Civil Code
24 § 1770, Plaintiffs and Class members have suffered and will continue to suffer injury,
25 ascertainable losses of money or property, and monetary and non-monetary damages, including
26 from fraud and identity theft; time and expenses related to monitoring their financial accounts for
27 fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of
28 their Private Information, including but not limited to the diminishment of their present and

1 future property interest in their Private Information and the deprivation of the exclusive use of
2 their Private Information.

3 189. Plaintiffs and the Class seek an order enjoining the acts and practices described
4 above.

5 **COUNT TWELVE**
6 **VIOLATION OF THE**
7 **CALIFORNIA CONSUMER PRIVACY ACT,**
8 **CAL. CIV. CODE §§ 1798.100, *ET SEQ.***

9 190. Plaintiffs, individually and on behalf of the Class, incorporate all foregoing
10 factual allegations as if fully set forth herein. This claim is brought individually under the laws of
11 California and on behalf of all other natural persons whose Private Information was
12 compromised as a result of the Data Breach.

13 191. Plaintiffs and Class members are residents of California.

14 192. AT&T is a corporation that is organized or operated for the profit or financial
15 benefit of its shareholders or other owners, with annual gross revenues over \$19 billion.

16 193. AT&T is a business that collects consumers' personal information as defined by
17 Cal. Civ. Code § 1798.140(e). Specifically, AT&T obtains, receives, or accesses consumers'
18 personal information when customers sign up for AT&T service.

19 194. On information and belief, AT&T is registered as a "data broker" in California,
20 which is defined as a "business that knowingly collects and sells to third parties the personal
21 information of a consumer with whom the business does not have a direct relationship." Cal. Civ.
22 Code § 1798.99.80.

23 195. AT&T violated Section 1798.150 of the California Consumer Privacy Act by
24 failing to prevent Plaintiffs and the Class members' nonencrypted and nonredacted personal
25 information from unauthorized access and exfiltration, theft, or disclosure as a result of AT&T's
26 violation of its duty to implement and maintain reasonable security procedures and practices
27 appropriate to the nature of the information.
28

196. AT&T knew or should have known that its data security practices were inadequate to secure the Class members' Private Information and that its inadequate data security practices gave rise to the risk of a data breach.

197. AT&T failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the Private Information it collected and stored.

198. The cybercriminals accessed “nonencrypted and unredacted personal information” as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d), in the Data Breach.

199. Upon information and belief, Plaintiffs and Class members' Private Information accessed by the cybercriminals in the Data Breach includes "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d).

200. Plaintiffs seeks injunctive relief in the form of an order requiring AT&T to employ adequate security practices consistent with law and industry standards to protect the Class members' Private Information, requiring AT&T to complete its investigation, and to issue an amended statement giving a detailed explanation that confirms, with reasonable certainty, what categories of data were stolen and accessed without the Class members' authorization, along with an explanation of how the data breach occurred.

201. Plaintiffs and the Class members seek statutory damages or actual damages, whichever is greater, pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

202. As a direct and proximate result of AT&T's violations of the Cal. Civ. Code §§ 1798.150, Plaintiffs and Class members suffered damages, as described above.

203. Plaintiffs and the Class seek pecuniary damages pursuant to Cal. Civil Code § 1798.150(b).

VII. PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and on behalf of the proposed Class, request that the Court:

a. Certify this case as a class action, appoint Plaintiffs as class representative, and appoint Plaintiffs' Counsel as Class Counsel for Plaintiffs to represent the Class;

b. Find that AT&T breached its duty to safeguard and protect the PII of Plaintiffs

CLASS ACTION COMPLAINT - 38

CASE NO.

and Class Members that was compromised in the Data Breach;

c. Award Plaintiffs and Class Members appropriate relief, including actual and statutory damages, restitution and disgorgement;

d. Award equitable, injunctive and declaratory relief as may be appropriate;

e. Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

f. Award pre-judgment and post-judgment interest as prescribed by law; and

g. Grant additional legal or equitable relief as this Court may find just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated April 19, 2024

Respectfully submitted,

COTCHETT PITRE & MCCARTHY LLP

/s/ Thomas E. Loeser

Joseph W. Cotchett (SBN 36324)

Andrew F. Kirtley (SBN 328023)

Gia Jung (SBN 340160)

San Francisco Airport Office Center

840 Malcolm Road, Suite 200

Burlingame, CA 94010

Telephone: (650) 697-6000

Fax: (650) 697-0577

jcotchett@cpmlegal.com

akirtley@cpmlegal.com

Gjung@cpmlegal.com

Thomas E. Loeser (CA SBN 202724)

Karin B. Swope

999 N. Northlake Way, Suite 215

Seattle, WA 98103

Tel: (206) 802-1272

Fax: (650) 697-0577

tloeser@cpmlegal.com

kswope@cpmlegal.com

Attorneys for Plaintiffs and the proposed Class